Federal Communications Commission
Washington, D.C. 20554

May 12, 2022

DA 22-488

Small Entity Compliance Guide

Promoting Technological Solutions to Combat
Contraband Wireless Device Use in Correctional Facilities

FCC 21-82
GN Docket No. 13-111
Released July 13, 2021

This Guide is prepared in accordance with the requirements of Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996. It is intended to help small entities—small businesses, small organizations (non-profits), and small governmental jurisdictions—comply with the revised rules adopted in the above-referenced Federal Communications Commission (FCC or Commission) rulemaking dockets. This Guide is not intended to replace or supersede these rules and, therefore, final authority rests solely with the rules. Although we have attempted to cover all parts of the rules that might be especially important to small entities, the coverage may not be exhaustive. This Guide cannot anticipate all situations in which the rules apply. Furthermore, the Commission retains the discretion to adopt case-by-case approaches, where appropriate, that may differ from this Guide. Any decision regarding a particular small entity will be based on the statute and relevant rules.

In any civil or administrative action against a small entity for a violation of rules, the content of the Small Entity Compliance Guide may be considered as evidence of the reasonableness or appropriateness of proposed fines, penalties or damages. Interested parties are free to file comments regarding this Guide and the appropriateness of its application to a particular situation. The FCC will consider whether the recommendations or interpretations in the Guide are appropriate in that situation. The FCC may decide to revise this Guide without public notice to reflect changes in the FCC's approach to implementing a rule, or it may clarify or update the text of the Guide. Direct your comments and recommendations, or calls for further assistance, to the FCC's Consumer Center:

1-888-CALL-FCC (1-888-225-5322)
TTY: 1-888-TELL-FCC (1-888-835-5322)
Videophone: 1-844-4-FCC-ASL (1-844-432-2275)
Fax: 1-866-418-0232

TABLE OF CONTENTS

I. OBJECTIVES OF THE PROCEEDING

This Small Entity Compliance Guide (SECG) is designed to help individuals and small businesses understand the requirements and other procedures for the Commission's process for obtaining approval of a Contraband Interdiction System (CIS) for use in the submission of qualifying requests for the disabling of contraband wireless devices in correctional facilities as established in the *Second Report and Order*.[1] This guide **is not a substitute** for reading and reviewing relevant orders, rules, and public notices, including the *Contraband Guidance Public Notice*,[2] nor is it a substitute for legal advice on how the rules apply to your circumstances.

In the *Second Report and Order* in GN Docket No. 13-111, *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, the Commission took further steps to facilitate the deployment and viability of technological solutions used to combat contraband wireless devices in correctional facilities. In some cases, incarcerated people use these devices to engage in a variety of criminal activities posing serious threats to officials and incarcerated people within the facility and innocent members of the public. In an Explanatory Statement to the 2021 Consolidated Appropriations Act, Congress urged the Commission to act on its 2017 *Further Notice of Proposed Rulemaking* in this proceeding and "adopt a rules-based approach . . . that would require immediate disabling by a wireless carrier upon proper identification of a contraband device."[3]

Consistent with Congress' guidance, in the *Second Report and Order*, the Commission adopted a framework requiring the disabling of contraband wireless devices detected in correctional facilities upon satisfaction of certain criteria.[4] The Commission further addressed issues involving oversight, wireless provider liability, and treatment of 911 calls. Finally, the Commission adopted rules requiring advance notice of certain wireless provider network changes to promote and maintain CIS effectiveness. In establishing rules requiring wireless providers to disable contraband wireless devices in correctional facilities and adopting a framework to enable designated correctional facility officials (DCFOs) relying on an authorized CIS to submit qualifying requests to wireless providers to disable contraband wireless devices in qualifying correctional facilities, the Commission found that a rules-based process will provide a valuable additional tool for departments of corrections to address contraband wireless device use. The framework includes a two-phase authorization process: (1) CIS applicants will submit applications to the Wireless Telecommunications Bureau (Bureau) describing the legal and technical qualifications of the systems; and (2) CIS applicants will perform on-site testing of approved CISs at individual correctional facilities and file a self-certification with the Commission. After both phases are complete, DCFOs will be authorized to

---

[1] *See In the Matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Second Report and Order and Second Further Notice of Proposed Rulemaking, 36 FCC Rcd 11813 (2021) (*Second Report and Order*); *see also In the Matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Erratum (rel. Aug. 3, 2021).

[2] *Wireless Telecommunications Bureau Provides Guidance for Filing Contraband Interdiction System Certification Applications and Self-Certifications*, GN Docket No. 13-111, Public Notice, DA 21-1572 (rel. Dec. 17, 2021) (*Contraband Guidance Public Notice*). The *Contraband Guidance Public Notice* provides guidance to stakeholders and additional details on the process for obtaining approval of a CIS for use in the submission of qualifying requests for the disabling of contraband wireless devices in correctional facilities.

[3] *See* Explanatory Statement to 2021 Consolidated Appropriations Act, Book IV, 166 Cong. Rec. H8311, H8440 (daily ed. Dec. 21, 2020) (2021 Explanatory Statement); *see also Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 2336 (2017).

[4] This framework and CIS authorization process is separate and distinct from, and does not replace, the process through which solutions providers historically have obtained authorization to operate CISs in correctional facilities by entering into lease arrangements with wireless providers.

submit qualifying requests to wireless providers to disable contraband devices using approved CISs at each correctional facility. In addition, the Commission adopted rules requiring wireless providers to notify certain types of CIS operators of major technical changes to ensure that CIS effectiveness is maintained. The Commission found that these rules will provide law enforcement with the tools necessary to disable contraband wireless devices, which, in turn, will help combat the serious threats posed by the illegal use of such devices.

II. COMPLIANCE REQUIREMENTS

A. CIS Certification Application Process and Procedures (47 CFR § 20.23(b)(1))[5]

CIS Certification Application Process. The first phase of the disabling framework requires a CIS applicant to submit a certification application to the Bureau for review and approval describing the legal and technical qualifications of the system that the applicant seeks to use as the basis for qualifying requests for contraband device disabling. The Bureau will base each certification determination on a demonstration that the CIS's overall methodology for system design and data analysis ensures, to the greatest extent possible, that only devices that are in fact contraband will be identified for disabling.

A CIS application must consist of two sections:

(1) *CIS Description.* CIS applicants must submit detailed showings and representations establishing that the systems are designed to minimize the risk of disabling a non-contraband wireless device; and

(2) *CIS Test Plan.* The Commission requires that an application for CIS certification include a test plan that can be adapted to the circumstances of each planned deployment at a specific correctional facility.

CIS Certification Application Filing Procedures. The CIS application must be signed by a duly authorized representative of the applicant and include a declaration in compliance with Commission rules.[6] Applications must be filed using the Commission's Electronic Comment Filing System (ECFS) and must refer to **GN Docket 13-111**. Applicants may request confidential treatment of information contained in their applications and should refer to the *Contraband Guidance Public Notice* for guidance on submitting confidential information.

Stakeholder Review of CIS Certification Applications. Stakeholders will have an opportunity to review and comment on the CIS certification applications prior to testing or deploying at a correctional facility. CIS applications found to be complete will be placed on public notice for review and comment. To review confidential filings, follow the procedures set forth in section 0.461 of the Commission's rules.[7] Once approved, the Bureau will maintain a publicly available list of certified CISs at https://www.fcc.gov/wireless/bureau-divisions/mobility-division/contraband-wireless-devices.

B. CIS Site-Based Testing and Self-Certification (47 CFR § 20.23(b)(3)-(6))

The second phase of the disabling framework requires CIS applicants to perform on-site testing of approved CISs at individual correctional facilities and file self-certifications with the Bureau confirming that the testing at a specific correctional facility is complete and was successful. A CIS operator—which could be a CIS solutions provider, or a DCFO or other responsible party that deploys its own CIS at a correctional facility—seeking to use the CIS to submit qualifying requests for disabling must test a certified

---

[5] For information on the dates of effectiveness of rules adopted in the Contraband *Second Report and Order*, see Section IV below.

[6] *See* 47 CFR §§ 1.16, 1.917 (for example, by one of the partners if the applicant is a partnership; or by an officer, director, or duly authorized employee, if the applicant is a corporation; or by a duly elected or appointed official who is authorized to do so under the laws of the applicable jurisdiction if the applicant is a government entity).

[7] *See* 47 CFR § 0.461 (detailing procedures for inspecting materials not routinely available for public inspection).

CIS, based on the previously approved test plan which was submitted with the CIS application. A CIS operator must test a certified CIS at **each** location where it intends to operate.

- Prior to initiating testing at a correctional facility, CIS operators must serve notice, in accordance with Commission rule section 1.47,[8] of the testing on all relevant wireless providers by email no later than seven business days before the date that testing will begin to give each such provider a reasonable opportunity to participate in the tests. The notice must include, at a minimum, the following information: (1) testing start and end date; (2) testing location; (3) testing parameters; and (4) contact information.

Thereafter, in order for the system to be used in the submission of qualifying requests at a specific correctional facility, the CIS operator must file a self-certification with the Bureau indicating that the testing at that correctional facility is complete and successful.

CIS Operator Self-Certification Filing Procedures. Following successful CIS testing, the CIS operator can refer to the *Contraband Guidance Public Notice*, which provides further guidance regarding the self-certification requirements.

- The self-certification submitted by a CIS operator must include a certification consistent with Commission rule section 1.16 and be accompanied by an attestation from the DCFO verifying that all information contained in the self-certification is true and accurate.
- The CIS self-certification must be filed using ECFS, and must refer to **GN Docket 13-111**.
- CIS operators must serve notice on all relevant wireless providers, in accordance with Commission rule section 1.47,[9] of the filing of the self-certification.

Wireless Providers Filing Objections to CIS Self-Certifications Procedures. Wireless providers have five business days from a self-certification filing date to submit objections to the Bureau, and any such objections must be served on the DCFO and the CIS operator.

- Wireless providers must file any objections to self-certifications through ECFS in **GN Docket No. 13-111**. In addition, in accordance with Commission rule section 1.47,[10] wireless providers must serve notice of the objection on the DCFO and the CIS operator when submitting the objection via ECFS.
- If a timely objection is submitted, the DCFO may not submit qualifying requests until the Bureau addresses the objection.
- If there are no objections, the DCFO may submit qualifying requests to wireless providers beginning on the sixth business day after the filing of the self-certification with the Bureau.
- A wireless provider may submit an objection to the Bureau after the five-day period lapses but must act on qualifying requests during the pendency of the objection.

Recertification Procedures. At least every three years after the initial self-certification, CIS operators seeking to maintain the ability to submit qualifying requests through a DCFO for contraband device disabling must retest their systems and recertify them for continued CIS accuracy. Recertifications must comply with the same rules and filing instructions that apply to the initial self-certification.

---

[8] 47 CFR § 1.47.

[9] *Id*.

[10] 47 CFR § 1.47(b), (f) ("[w]here any person is required to serve any document filed with the Commission, service shall be made by that person or by his representative on or before the day on which the document is filed").

Suspension. The Bureau may suspend a CIS certification generally or at a particular facility if subsequent credible information calls into question a system's reliability.

C. Designated Correctional Facility Official Requirements (47 CFR § 20.23(c)(1))

The rules adopted by the Commission require that qualifying disabling requests be submitted by an official of the state, local, or federal government entity responsible for administration and oversight of the relevant correctional facility, who is a qualified DCFO.

- Any person meeting the DCFO definition that seeks authority to submit qualifying requests must send a letter, addressed to the Commission's Contraband Ombudsperson, signed by the relevant state attorney general or, if a federal correctional facility, the relevant Bureau of Prisons Regional Director, that provides the individual's name, official government position, and a list of correctional facilities over which the individual has oversight and management authority. The letter must be addressed to Charles Mathias, Contraband Ombudsperson, Federal Communications Commission, 45 L Street, NE, Washington, DC 20554.
- Prospective DCFOs must file the required letter via ECFS and refer to **GN Docket No. 13-111**.
- Once approved, the Bureau will maintain a publicly available list of approved DCFOs authorized to transmit qualifying disabling requests at https://www.fcc.gov/wireless/bureau-divisions/mobility-division/contraband-wireless-devices.[11]

D. Disabling Contraband Wireless Devices Procedures (47 CFR § 20.23(c)(1)-(4))

The procedures adopted by the Commission for disabling contraband wireless devices allow a DCFO to request that a CMRS licensee disable a contraband wireless device that has been detected in a correctional facility by a certified CIS.

- Once a CIS operator is certified and absent objections from wireless providers, a DCFO may submit a qualifying request to a wireless provider beginning on the sixth business day after the later of the self-certification filing or actual service.
- A qualifying request submitted by a DCFO must be made in writing and include certifications as outlined in the Commission's rules. The certifications must include a list of the contraband devices, with identifiers sufficient to uniquely describe the devices at both the subscription and device-levels, to provide the wireless provider with the information necessary to prevent use of contraband devices on its network and on other wireless provider networks.

Licensee Actions Upon Receipt of a Qualifying Request. After the DCFO submits the request to disable a contraband wireless device, the licensee must verify that the request contains the required information. The licensee must then follow the rules in 47 CFR § 20.23 regarding disabling a contraband device or rejecting a qualifying request.[12]

---

[11] Consistent with the Privacy Act, by submitting this letter, the individual seeking DCFO designation consents to their name, title, and related correctional facilities, as described in this paragraph, being made publicly available on the Commission's website. 5 U.S.C. § 552a.

[12] *See* 47 CFR § 20.23 (Disabling contraband wireless devices). On September 9, 2021, CTIA filed a petition for partial reconsideration of the *Second Report and Order* seeking a modification of the two-day contraband wireless device disabling timeframe required pursuant to section 20.23(c)(3)(i) of the Commission's rules. *See* Comments of CTIA on Second Further Notice of Proposed Rulemaking and Petition for Partial Reconsideration, GN Docket No. 13-111 (filed Sept. 9, 2021) (CTIA Petition). The CTIA Petition is pending Commission review.

Notification Requirements. A licensee is not required to conduct customer outreach before disabling a contraband wireless device, but may contact the customer of record. The licensee must inform the DCFO whether the qualifying request has been granted or rejected within two business days of receiving the qualifying request.

Reversals. A wireless provider may reverse the disabling of the wireless device where the licensee determines that the wireless device was erroneously identified as contraband. The following rules are applicable to the reversal of a wireless device that has been disabled:

- A wireless provider may request that a DCFO review and confirm the information provided in the qualifying request prior to reversing the disabling action. The DCFO should review and respond to the request.
    - If the DCFO directs the wireless provider to reverse the disabling request, the wireless provider must restore the device within two business days of receipt of the response.
    - If the DCFO fails to respond to the wireless provider within two business days, the wireless provider may reverse the disabling action.
- DCFOs must provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices on a quarterly basis at the end of any quarter during which a device disabling was reversed. The *Contraband Guidance Public Notice* contains filing instructions for providing notice to the Contraband Ombudsperson.

E. Notification to Managed Access System (MAS) Operators (47 CFR § 20.23(d))

The rules adopted by the Commission require wireless providers to provide advance notice to MAS operators of certain technical network changes in order to ensure the ongoing effectiveness of MAS.

- 90 days advance notice is required for limited categories of major network changes occurring within 15 miles of a correctional facility with an authorized MAS, unless parties modify notification arrangements through mutual agreement or if the network technical changes are required due to emergency or disaster preparedness. CMRS licensees must provide notice of these technical changes immediately after the exigency.
- CMRS licensees and MAS operators are required to negotiate in good faith to reach an agreement for notification for those types of network adjustments that are more frequent, localized wireless provider network changes and are not covered by the notice requirement.

III. RECORDKEEPING AND REPORTING REQUIREMENTS

CIS operators must retain and make available upon Bureau request the records of all information supporting each request for device disabling, and the basis for disabling each device for at least five years following the date of submission of the relevant disabling request (47 CFR § 20.23(b)(7)). In addition, DCFOs must provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices on a quarterly basis at the end of any quarter during which a device disabling was reversed (47 CFR § 20.23(c)(4)(v)).

IV. IMPLEMENTATION DATE

Rule sections 20.3; 20.23(b)(2), (4), (6); (c)(3)(i)-(ii), (4)(iii)-(iv) became effective on September 13, 2021. Rule sections 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d) are subject to the Paperwork Reduction Act (PRA) requiring Office of Management and Budget (OMB) approval, and do not take effect until they are approved by OMB, and the Commission publishes a document in the Federal Register announcing the effective date. On May 3, 2022, the required document was published in the Federal Register indicating that the above-referenced rules were to take effect immediately.

On May 3, 2022, the Bureau simultaneously released two separate Public Notices indicating that: (1) the rules requiring PRA approval went into effect on May 3, 2022; and (2) the Bureau would immediately begin accepting applications for CIS certification and letters requesting DCFO status.[13]

V. INTERNET LINKS

A copy of the *Second Report and Order* is available at:

https://www.fcc.gov/document/fcc-requires-disabling-contraband-phones-correctional-facilities.

A copy of the *Second Report and Order Erratum* is available at:

https://docs.fcc.gov/public/attachments/DOC-374609A1_Erratum.docx.

A copy of the *Federal Register* Summary of the *Second Report and Order* is available at:

https://www.govinfo.gov/content/pkg/FR-2021-08-13/pdf/2021-15748.pdf.

A copy of the *Contraband Guidance Public Notice* is available at:

https://www.fcc.gov/document/wtb-guidance-filing-contraband-interdiction-system-certifications.

A copy of the *Federal Register* publication announcing OMB approval of the final rules subject to PRA, and the effective date of these rules is available at:

https://www.govinfo.gov/content/pkg/FR-2022-05-03/pdf/2022-09203.pdf.

Additional helpful information is available at:

https://www.fcc.gov/wireless/bureau-divisions/mobility-division/contraband-wireless-devices.

[13] *See* Wireless Telecommunications Bureau Announces Effective Date for Certain Contraband Interdiction System Rules, GN Docket No. 13-111, Public Notice, DA 22-474 (May 3, 2022); Wireless Telecommunications Bureau Begins Accepting Contraband Interdiction System Certification Applications and Designated Correctional Facility Official Requests, GN Docket No. 13-111, Public Notice, DA 22-475 (May 3, 2022).